株式会社ゼンショーホールディングス 御中

スマートフォンアプリケーション診断
(Android/iOS)
結果報告書

オリーブの丘

2023年9月

三井物産セキュアディレクション株式会社

目次

1. はじめに

この度は、私ども、三井物産セキュアディレクション株式会社(以下、弊社)にセキュリティ診断をご用命いただきありがとうございました。診断を完了いたしましたので、その結果についてご報告させていただきます。

本報告書には、診断で検出した事項についての事象の説明に加え、考えられる影響や、対策方法などについても記載しております。対策方針の検討や対策の実施にご活用いただければ幸いです。

なお、本報告書には、貴社のセキュリティ上の脆弱性に関わる情報などの重要な情報が含まれております。情報の重要度レベルにあった適切なお取り扱いをお願いするとともに、閲覧、複写などに対しても十分ご留意いただき、不必要な情報の拡散が発生しないよう、慎重に取り扱っていただきますようお願い申し上げます。万一、ご納品後に本報告書の内容が漏れたことに関する問題が発生した場合について、弊社ではその責任を負いかねますのであらかじめご了承ください。

2. 診断概要

2-1. リスク評定方法

検出したそれぞれの脆弱性に対し、業務への影響度などを考慮し、4 段階(**High**、**Medium**、**Low**、**Info**)のリスク評定を行います。具体的な評定基準は巻末の Appendix.2 危険度判定基準の表に示しましたのでご参照ください。検出した脆弱性に対する評定は弊社独自の見解であり、推測を含む場合があります。貴社にとって最適なものであるかをご確認ください。

2-2. 実施概要

・診断対象

オリーブの丘

[Android]

ファイル名：app.apk

バージョン：2.0.0

MD5ハッシュ：fd53c720c239af7ebf4c4537d490da80

[iOS]

ファイル名：app.ipa

バージョン：5.0.0

MD5ハッシュ：df112c6d86004dec6eb6d667c83af7da

・診断期間

2023/8/14 ～ 2023/9/1

・診断手法

手動/ツールによるブラックボックス診断

(診断項目一覧はAppendix.1を参照)

・診断形態

インターネット経由のリモート診断

・使用 IP アドレス

113.43.174.224/29
153.150.126.144/29
150.249.228.96/28
114.156.13.240/28
114.156.142.98/32

・備考

–

3. 総合評価

3-1. 評価

" B "危険度 Medium の脆弱性を検出

評価	説明
S	脆弱性が検出されず非常にセキュアな状態
A	危険度 Low の脆弱性のみを検出
B	危険度 Medium の脆弱性を検出
C	危険度 High の脆弱性を検出
D	危険度 High の脆弱性を複数種類検出

(個別脆弱性の危険度判定基準はAppendix.2を参照)

3-2. 総評

診断の結果、危険度Mediumの脆弱性が1件、危険度Lowの脆弱性が2件検出されました。全体評価はBとなります。

Androidアプリケーションでは、サーバとの暗号化通信を確立する際に行われるサーバ証明書の検証に不備がある危険度Medium「通信処理におけるSSLサーバ証明書検証の不備」の脆弱性を確認しております。WebViewで検出した通信においては、意図しないサーバ証明書を受け取った場合は、「SSL Certificate Error, The certificate authority is not trusted. Do you want to continue anyway?」などのメッセージを含むダイアログが表示され、通信を継続するか否かのユーザ操作が必要となる仕組みを実装されています。しかしながら、ユーザが正当なサーバ以外との通信を許可してしまうと、中間者攻撃により通信で扱う重要情報の漏えいや改ざんが行われる可能性があります。安全な通信を確立するためにも、ダイアログによるユーザ選択の操作を取りやめ、サーバ証明書の発行元並びにホスト名を検証するよう対策されることを推奨します。

また、待ち順確認として利用されるQRコードの検証に不備があるため、任意のWebページがアプリケーション内に表示されフィッシングなどに悪用される脆弱性を検出しています。意図しないWebページが表示されないよう読み込む文字種を限定した上で入力値検証をおこなうなどの対策をご検討ください。

その他、AndroidおよびiOS共に本アプリケーションで扱うポイント移行用のIDやセッションIDなどの重要情報を端末内に平文で保存されている問題を確認しています。攻撃者が該当情報を参照するには、端末に物理的にアクセスする必要があるため、一定のハードルがあるものの安全にデータを管理するためにも不要な情報は出力しない、あるいは暗号化して保存するといった対策をご検討することを推奨します。

今回検出されたすべての報告事項の一覧並びに詳細は次章に記載しております。内容をご確認の上、対策の要否についてご検討ください。

4. 検出事項

4-1. 検出事項一覧

検出された脆弱性一覧を以下に示します。リスク評定方法については「Appendix.2 危険度判定基準」をご参照ください。

■ Android

No	危険度	名称	ページ
1	Medium	通信処理における SSL サーバ証明書検証の不備	7
2	Low	QR コードの検証不備	9
3	Info	ローカルファイルに重要情報が平文で保存される	11
4	Info	ローカルファイル(Cache)に重要情報が平文で保存される	12
5	Info	ローカルファイルにセッション ID が平文で保存される	14
6	Info	不要なログ出力	16
7	Info	ログアウト機能の欠如	18
8	Info	不必要な画面遷移	19
9	Info	開発時の情報を保存及び内包	21

■ iOS

No	危険度	名称	ページ
1	Low	ローカルファイルに重要情報が平文で保存される	23
2	Info	ローカルファイル(Cache)に重要情報が平文で保存される	24
3	Info	ローカルファイルにセッション ID が平文で保存される	27
4	Info	ログアウト機能の欠如	28
5	Info	端末内に重要情報などを含むスナップショットを保存	29
6	Info	不必要な画面遷移	31
7	Info	実行ファイル内に内部パスが含まれている	33
8	Info	開発時の情報を保存及び内包	35

(個別脆弱性の危険度判定基準はAppendix.2を参照)

4-2. 脆弱性詳細

報告番号:«ZNSH-app-1»

[1] 通信処理における SSL サーバ証明書検証の不備

危険度 Medium

Android

・想定される影響

通信経路上の攻撃者によって通信内容を窃取または改ざんされる可能性がある。

・解説

SSL通信時のサーバ証明書の検証に不備があり、正当なサーバ以外でも接続を確立する。

▼事例. サーバ証明書、及びサーバ証明書のホスト名
本アプリケーションのWebView通信において、意図していないサーバ証明書やサーバ証明書のホスト名を受け取ると「SSL Certificate Error, The certificate authority is not trusted. Do you want to continue anyway?」などのダイアログが表示される。しかしながら、ユーザが通信を許可することで任意のSSLサーバ証明書を受けつけてしまうため、中間者攻撃される可能性がある。

以下は、本アプリケーションのWebView通信のうち、メイン機能であるホームタブの「持ち帰り注文」と「メニュータブ」をタップした際ににSSLサーバ証明書を検証していないFQDNの一部である。

- www.olivenooka.jp
- takeout.olivenooka.jp
- ajax.googleapis.com
- www.googletagmanager.com
- stats.g.doubleclick.net
- analytics.google.com
- www.google-analytics.com
- code.jquery.com

▼対象
メニュータブ
店舗検索タブ 検索実施 店舗詳細
ハンバーガーメニュー よくある質問
ハンバーガーメニュー その他のお問い合わせ
ハンバーガーメニュー 利用規約
ハンバーガーメニュー 個人情報保護方針
ホーム オリーブの丘は毎日10:00オープン!
ホーム コンセプト
ホーム メニュー
ホーム お持ち帰りメニュー
ホーム Uber Eats
ホーム 出前館
ホーム アルバイトスタッフ大募集！
ホーム　バナー（広告）オリーブの丘(Webページ)
会員証　「?」アイコン　詳しい内容はHPをご確認ください。

・対策

SSLサーバ証明書の発行元並びにホスト名を検証する。

・備考

－

報告番号:«ZNSH-app-2»

[2] QR コードの検証不備

危険度 Low

Android

・想定される影響

ページの見かけ上の改ざんによるフィッシングなどに悪用される可能性がある。

・解説

本アプリケーションでは、待ち順確認用のQRコードをスキャンすることで待ち順状態を確認できる機能がある。

以下は、待ち順確認として利用されるQRコード値の例である。
[待ち順確認用のQRコードの例]

```
https://stag.z-navi.com/status-check.html?qr=ZNV6846654098000000043000p9982
02308231127
```

なお、本アプリケーションが該当のQRコードを処理するには以下の条件を満たしている必要がある。

▼条件
(1) QRコードに「https://stag.z-navi.com/status-check.html?qr=」の文字列が含まれている
(2) 条件(1)のURLのクエリパラメータ(qr)で利用される文字列長が21文字より長い

しかしながら、待ち順を確認するQRコードの検証に不備があるため任意のWebページを本アプリケーションのWebViewに表示させることが可能である。

▼再現例
攻撃者が不正なQRコードを作成した上で、被害者を誘導し該当のQRコードをスキャンさせることで不正なサイトへ遷移させることが可能である。

1. 攻撃者は以下のような文字列を含むQRコードを作成する。

[不正なQRコードの例]

```
https://www.mbsd.jp?x=https://stag.z-navi.com/status-check.html?qr=ZNV6846654
09800000043000p998202308231127
```

2. 攻撃者は被害者を誘導し、手順(1)で作成したQRコードをスキャンさせる。
3. QRコードスキャン後、QRコードに含まれるURLのホスト(www.mbsd.jp)にアクセスするため該当のページがWebviewに表示される。

▼対象
ホームタブ 待ち順確認

・対策

読み込むQRコードの文字列にURLを含めず、待ち順確認で用いる値のみに限定する。加えて、入力値検証を行い利用する文字種以外はエラーとする。

・備考

－

報告番号:«ZNSH-app-3»

[3] ローカルファイルに重要情報が平文で保存される

危険度 Info

Android

・想定される影響

ポイント移行用のIDが漏えいする可能性がある。

・解説

本アプリケーションでは、重要情報であるポイントの移行用のIDが端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、当該情報が漏えいする可能性がある。

▼事例. ポイント移行用のID
以下は、本アプリケーションで獲得したポイントを移行するために利用されるIDが平文で保存されるローカルファイルの該当箇所である。
[<Application Data>/shared_prefs/oln_app_dev.xml の内容(抜粋)]

```
<string name="MERGE_CODE">PPWV2308211457247</string>
<boolean name="CLOSED_WARNING" value="true" />
```

▼対象
<Application Data>/shared_prefs/oln_app_dev.xml

・対策

以下のいずれかの対策を実施する。
- 端末内に重要情報を保存しないようにする
- 端末内に重要情報を保存する場合は、平文ではなく暗号化して保存する
- アプリケーションの終了時などに該当するローカルファイルを削除する

・備考

本アプリケーションでは、AndroidManifest.xmlファイルにてバックアップの取得を禁止(allowBackup="false")しているため、当該ファイルの参照には管理者権限が必要となる。ただし、攻撃者が端末を窃取又は拾得した後に管理者権限でアクセスするためにroot化を実行する可能性もあるため、対策することを推奨する。

報告番号:«ZNSH-app-17»

[4] ローカルファイル(Cache)に重要情報が平文で保存される

危険度 Info

Android

・想定される影響

利用者の名前、電話番号とメールアドレスが漏えいする可能性がある。

・解説

本アプリケーションでは、利用者の名前やメールアドレスなどの重要情報がキャッシュとして端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、当該情報が漏えいする可能性がある。

▼事例. 利用者の名前、電話番号、メールアドレス
以下は、利用者の名前、電話番号とメールアドレスが平文で保存されるローカルファイルの該当箇所である。

<Application Data>/cache/WebView/Default/HTTP Cache/Cache_Data/64f90e6996f388a7_0の内容(抜粋)]

```
00003100  20 20 20 20 20 20 20 20  20 20 20 3c 74 64 20 69  |           <td i|
00003110  64 3d 22 73 74 65 70 30  30 35 5f 30 34 5f 74 65  |d="step005_04_te|
00003120  78 74 30 31 22 3e 4d 69  74 73 75 69 20 54 61 72  |xt01">Mitsui Tar|
00003130  6f 75 3c 2f 74 64 3e 0a  20 20 20 20 20 20 20 20  |ou</td>.        |
...(省略)...
000031c0  20 20 20 20 20 20 20 20  20 20 20 20 20 3c 74 64  |             <td|
000031d0  20 69 64 3d 22 73 74 65  70 30 30 35 5f 30 34 5f  | id="step005_04_|
000031e0  74 65 78 74 30 32 22 3e  30 33 35 36 34 39 31 39  |text02">03564919|
000031f0  36 31 3c 2f 74 64 3e 0a  20 20 20 20 20 20 20 20  |61</td>.        |
...(省略)...
00003290  20 20 20 20 20 20 3c 74  64 20 69 64 3d 22 73 74  |      <td id="st|
000032a0  65 70 30 30 35 5f 30 34  5f 74 65 78 74 30 33 22  |ep005_04_text03"|
000032b0  3e 77 65 62 73 65 63 36  35 39 40 70 73 2e 6d 62  |>websec659@ps.mb|
000032c0  73 64 2e 6a 70 3c 2f 74  64 3e 0a 20 20 20 20 20  |sd.jp</td>.     |
```

▼対象
<Application Data>/cache/WebView/Default/HTTP Cache/Cache_Data/64f90e6996f388a7_0
※ファイル名は都度変わる

・対策

以下のいずれかの対策を実施する。

・　キャッシュデータを端末内に保存しないようにする

・　アプリケーションの終了時などに該当するキャッシュファイルを削除する

・備考

当該ファイルの参照には、管理者権限が必要となる。ただし、攻撃者が端末を窃取又は拾得した後に管理者権限でアクセスするためにroot化を実行する可能性もあるため、対策することを推奨する。

報告番号:«ZNSH-app-4»

[5] ローカルファイルにセッション ID が平文で保存される

危険度 Info

Android

・想定される影響

有効なセッションIDが漏えいした場合、正規のユーザになりすました攻撃者によってサービスを不正に利用される可能性がある。

・解説

本アプリケーションでは、セッションID(Bearer, fueldid)が端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、セッションIDが漏えいする可能性がある。

▼事例1. セッションID(Bearer)
以下は、サーバ(stg.coupons-api.zensho.com)との間で利用されているセッションID(Bearer)が平文で保存されるローカルファイルの該当箇所である。

[<Application Data>/shared_prefs/oln_app_dev.xmlの内容(抜粋)]

```
<string name="BEARER_TOKEN_KEY">381703611f77159a62b94f7c1d701a6471a4dec510953578ed130e2d1d7c9476</string>
<boolean name="IS_LOGIN" value="true" />
```

▼対象1
<Application Data>/shared_prefs/oln_app_dev.xml

▼事例2. セッションID(fueldid)
以下は、持ち帰り注文を行う際にサーバ(takeout.olivenooka.jp)との間で利用されるセッションID(fueldid)が平文で保存されるローカルファイルの該当箇所である。

[<Application Data>/app_webview/Default/Cookiesの内容(抜粋)]

```
13338459585612972|takeout.olivenooka.jp||fueldid|S%3Ax62PYOyWLXeMnx_NicAOeKKH-GFZJS_GMcp07VTgj622sSwmDOOD7QlXyD49hflBemhv6RYrEPekUyS41wl8AhYlfmzWGvqB5M0bPyJR8fuptoYUgpmfyEjZSzJhlCsG9WdDfNhoHZHfFtca2JByP7N-1UJIXwSASazwktQC4YzUDpnoswZkhLHQu75ZeYyVgTojogB_RI1yu9UC1jv8YeExcTbPk0HXMxA%3D||/|13338466785612972|0|0|13338459585612972|1|1|1|-1|2|443|0|13338459585613134
13338459579694626|takeout.olivenooka.jp||lat[0]|35.6852807||/|13341051579694607|0|0|13338459579694626|1|1|1|-1|2|443|0|13338459579694626
```

▼対象2
<Application Data>/app_webview/Default/Cookies

・対策

以下のいずれかの対策を実施する。

- 端末内に認証情報を保存しないようにする
- 端末内に認証情報を保存する場合は、平文ではなく暗号化して保存する
- アプリケーションの終了時などに該当するローカルファイルを削除する

・備考

－

報告番号:«ZNSH-app-5»

[6] 不要なログ出力

危険度 Info

Android

・想定される影響

アプリケーションの挙動解析の手掛かりとなる可能性がある。

・解説

本アプリケーションでは、エラー発生時のスタックトレースをログに出力している。このため、仮に攻撃者により端末に物理的にアクセスされログを参照された場合、アプリケーションの挙動解析の手掛かりとなる情報が漏えいする可能性がある。

▼事例. スタックトレース
以下は、本アプリケーション起動時に出力されたログの例である。

[出力されたログ(抜粋)]

```
W/System.err( 2702): java.lang.NullPointerException: Attempt to invoke interface method 'java.lang.Object[] java.util.Collection.toArray()' on a null object reference
W/System.err( 2702):        at java.util.ArrayList.<init>(ArrayList.java:191)
W/System.err( 2702):        at jp.co.zensho.olivenooka.home.HomeFragment.J(:6)
W/System.err( 2702):        at i.a.a.a.q.z$a.J(:2)
W/System.err( 2702):        at i.a.a.a.q.y$a.d(:2)
W/System.err( 2702):        at d.a.a.a.a.d.a(:30)
W/System.err( 2702):        at n.m$b$a.d(Unknown Source:25)
W/System.err( 2702):        at n.a.run(Unknown Source:6)
W/System.err( 2702):        at android.os.Handler.handleCallback(Handler.java:942)
W/System.err( 2702):        at android.os.Handler.dispatchMessage(Handler.java:99)
W/System.err( 2702):        at android.os.Looper.loopOnce(Looper.java:201)
W/System.err( 2702):        at android.os.Looper.loop(Looper.java:288)
W/System.err( 2702):        at android.app.ActivityThread.main(ActivityThread.java:7872)
W/System.err( 2702):        at java.lang.reflect.Method.invoke(Native Method)
W/System.err( 2702):        at com.android.internal.os.RuntimeInit$MethodAndArgsCaller.run(RuntimeInit.java:548)
W/System.err( 2702):        at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:936)
```

▼対象
アプリケーション全体

・対策

重要な情報やスタックトレース等の不要な情報をログに出力しない。

・備考

報告した箇所以外でも同様の問題が発生する可能性があるため、対策する際は全体を見直すことを推奨する。

報告番号:«ZNSH-app-6»

[7] ログアウト機能の欠如

危険度 Info

Android

・想定される影響

有効なセッションIDが漏えいした場合、正規のユーザになりすました攻撃者によってサービスを不正に利用される可能性がある。

・解説

本アプリケーションに実装されているログアウト処理に不備がある。

本アプリケーションにはログイン機能が実装されているものの、ログアウト機能は実装されておらず、ユーザが明示的にログアウトすることができない。このため、何らかの原因でセッションIDが漏えいした場合、そのセッションIDを用いてサーバにアクセスされることで、正規のユーザになりすましてサービスを不正に利用される可能性がある。

▼対象
アプリケーション全体

・対策

ユーザが明示的にセッションを無効にできるよう、ログアウト機能を実装する。

・備考

–

報告番号:«ZNSH-app-7»

[8] 不必要な画面遷移

危険度 Info

Android

・想定される影響

- ユーザが入力した情報がローカルファイルに平文で保存される可能性がある
- 不正なサイトへアクセスする可能性がある

・解説

サービス外のWebページを本アプリケーションのWebViewに表示可能である。

本アプリケーションでは、オリーブの丘のWebページ(www.olivenooka.jp)に表示されているSNSアカウントのリンクなどから任意のWebページを本アプリケーションのWebView上で表示できる。このため、WebViewに表示されたWebページ上で検索文字列や認証に利用する文字列を入力すると、それらの情報がローカルファイルに意図せず保存される可能性がある。また、ブラウザとは異なりWebViewでは表示されるサイトのURLは画面に表示されず、ユーザが不正なサイトにアクセスしたことに気づきにくいため、フィッシングなどの被害を受ける可能性もある。

▼対象
メニュー　オリーブの丘(Webページ)
店舗検索　お近くの店舗／店舗を調べる　オリーブの丘(Webページ)
ハンバーガーメニュー よくある質問
ハンバーガーメニュー その他のお問い合わせ
ハンバーガーメニュー 利用規約
ハンバーガーメニュー 個人情報保護方針
初回起動時 利用規約
新規登録　利用規約
新規登録　個人情報保護方針
ホーム お持ち帰り注文 公式サイトへ
ホーム　バナー（広告）オリーブの丘(Webページ)
ホーム オリーブの丘は毎日10:00オープン!
ホーム コンセプト
ホーム メニュー
ホーム お持ち帰りメニュー
ホーム Uber Eats
ホーム 出前館
ホーム アルバイトスタッフ大募集！
会員証　「?」アイコン　詳しい内容はHPをご確認ください。

・対策

本アプリケーションのWebViewに表示するアクセス先URLを制限する。又は、本アプリケーションのサービスに不必要なURLについてはブラウザを利用する。

・備考

記載した対象以外でも同様の問題が発生する可能性があるため全体を見直すことを推奨する。

報告番号:«ZNSH-app-8»

[9] 開発時の情報を保存及び内包

危険度 Info

Android

・想定される影響

- 開発に利用しているサーバ(開発環境)に、外部から不正にアクセスされる可能性がある。
- ポイント獲得用のQRコードが漏えいすることで不正利用される可能性がある。

・解説

本アプリケーションの実行ファイルには、開発用のIPアドレスやポイント獲得用のQRコードがハードコードされている。このため、実行ファイルを解析され該当情報が漏えいすると不正アクセスや悪用される可能性がある。

▼事例1. 開発用IPアドレス
以下は、開発で利用されていると思われるIPアドレスの情報が保存されているファイルの該当箇所である。

[<APK>/res/xml/security_config.xmlの内容(抜粋)]

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        ...(省略)...
        <domain includeSubdomains="true">52.68.217.122
        </domain>
        <domain includeSubdomains="true">54.64.74.199
        </domain>
        <domain includeSubdomains="true">54.64.59.18
        </domain>
        <domain includeSubdomains="true">3.115.201.116
        </domain>
    </domain-config>
</network-security-config>
```

▼対象1
<APK>/res/xml/security_config.xml

▼事例2.　ポイント獲得用のQRコード
以下は、ポイント獲得用のQRコードとして利用される文字列が実行ファイルにハードコードされているクラス(jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity)の該当箇所の例である。

[jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivityの例(抜粋)]

```
public /* synthetic */ void t0(View view) {
    l0("RJPQvq+qEwbkHDaIhkB4F8esLND83PxbDz2NtTh+B9fw+Q=OySqH38PmFDzPkgzgqV/Pw==");
}
```

上記の値において、サーバ(stg.coupons-api.zensho.com)に問い合わせて有効性を確認した結果、無効であったものの将来的に有効値として利用されている場合も考えられる。

▼対象
・APKファイル(クラス)
　jp.co.zensho.olivenooka.rankup.scanqrcode.MLKitScanQRCodeRankUpActivity
　jp.co.zensho.olivenooka.rankup.scanqrcode.ScanQRCodeRankUpActivity

・対策

リリース版のアプリケーションにおいて不要な情報やファイルは削除する。

・備考

－

報告番号:«ZNSH-app-9»

[10] ローカルファイルに重要情報が平文で保存される

危険度 Low

iOS

・想定される影響

ポイント移行用のIDが漏えいする可能性がある。

・解説

本アプリケーションでは、ポイント移行用のIDが端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、当該情報が漏えいする可能性がある。

▼事例. ポイント移行用のID
以下は、本アプリケーションで獲得したポイントを移行するために利用されるIDが平文で保存されるローカルファイルの該当箇所である。

[<Application Home>/Preferences/oln_app_dev.xml の内容(抜粋)]

```
<key>merge_point_code</key>
<string>PUDJ2308091602017</string>
```

▼対象
<Application Home>/Preferences/jp.co.zensho.olivenooka.stg.plist

・対策

以下のいずれかの対策を実施する。

- 端末内に重要情報を保存しないようにする
- 端末内に重要情報を保存する場合は、平文ではなく暗号化して保存する
- アプリケーションの終了時などに該当するローカルファイルを削除する
- アプリケーション領域内に保存せずkeychainに保存する

・備考

－

報告番号:«ZNSH-app-10»

[11] ローカルファイル(Cache)に重要情報が平文で保存される

危険度 Info

iOS

・想定される影響

- 氏名や電話番号などの重要情報が漏えいする可能性がある。
- 有効なセッションIDが漏えいした場合、正規のユーザになりすました攻撃者によってサービスを不正に利用される可能性がある。

・解説

本アプリケーションでは、氏名や電話番号などの重要情報がキャッシュとして端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、当該情報が漏えいする可能性がある。

▼事例1. 氏名や電話番号、セッションIDなど
以下は、持ち帰り注文のテイクアウト弁当WEB注文画面で入力したお客様情報(氏名や電話番号、メールアドレス)が平文でキャッシュとして保存されているローカルファイルの該当箇所である。加えて、該当処理で利用しているセッションID(fueldid)もキャッシュとして保存されている。

[出力されたレスポンス(抜粋)]

```
<div class="info_block">
<p class="info_block_title">お客様情報</p>
<!-- #step005_04 -->
<div id="step005_04">
  <!-- .info_block_table -->
  <table class="info_block_table">
    <tbody><tr>
      <th>お名前</th>
      <td id="step005_04_text01">TANAKA Ichirou</td>
    </tr>
    <tr>
      <th>電話番号</th>
      <td id="step005_04_text02">08010127251</td>
    </tr>
    <tr>
      <th>メールアドレス</th>
      <td id="step005_04_text03">websec181@ps.mbsd.jp</td>
    </tr>
  </tbody></table>
  <!-- /.info_block_table -->
</div>
```

```
<!-- /#step005_04 -->
</div>
```

▼対象1
<Application Home>/Library/Caches/WebKit/NetworkCache/Version 16/Blobs/75EDDAA05F3B7731B31F5EDD969475847E93171A
<Application Home>/Library/Caches/WebKit/NetworkCache/Version 16/Records/9B06CFFF7145CDE8D732B7282CA6E1E8503CDEEF/Resource/20D0D6057CE5AA97D3E270E11D20307B2DBAA508-blob
※Records以下のディレクトリ名とファイル名は都度変わる

▼事例2. セッションID(Bearer)
以下は、サーバ(map-api.zensho.com、stg.coupons-api.zensho.com)との通信で利用されるセッションID(Bearer)が平文で保存されるローカルファイルの該当箇所である。
[<Application Home>/Library/Caches/jp.co.zensho.olivenooka.stg/Cache.db-walの内容(一部抜粋)]

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
	<key>Version</key>
	<integer>9</integer>
	<key>Array</key>
	<array>
		<false/>
		<dict>
			<key>_CFURLStringType</key>
			<integer>15</integer>
			<key>_CFURLString</key>
			<string>https://map-api.zensho.com/webapi/now?brand_id=39&amp;distance=20000&amp;lat=35.68347720945734&amp;limit=100&amp;lng=139.7844892793473&amp;offset=0</string>
		</dict>
		<real>60.000000</real>
		<integer>0</integer>
・・・（省略）・・・
			<key>User-Agent</key>
			<string>Olivenooka_Stg/5.0.0 (jp.co.zensho.olivenooka.stg; build:1; iOS 14.6.0) Alamofire/5.6.4</string>
			<key>Authorization</key>
```

<string>Bearer 3113adeb24f830054f14345846a87b1d21868235b8a15c3fc85dde5747a972ca</string>
<key>Accept-Language</key>
<string>ja-JP;q=1.0</string>
<key>Accept-Encoding</key>
<string>br;q=1.0, gzip;q=0.9, deflate;q=0.8</string>
</dict>
<string>__CFURLRequestNullTokenString__</string>
<string>__CFURLRequestNullTokenString__</string>
</array>
</dict>
</plist>

▼対象2
<Application Home>/Library/Caches/jp.co.zensho.olivenooka.stg/Cache.db
<Application Home>/Library/Caches/jp.co.zensho.olivenooka.stg/Cache.db-wal

・対策

以下のいずれかの対策を実施する。
・ キャッシュデータを端末内に保存しないようにする
・ アプリケーションの終了時などに該当するキャッシュファイルを削除する

・備考

当該ファイルの参照には、管理者権限が必要となる。ただし、攻撃者が端末を窃取、又は拾得した後に管理者権限でアクセスするためにJailBreakを実行する可能性もあるため、対策することを推奨する。

報告番号:«ZNSH-app-11»

[12] ローカルファイルにセッション ID が平文で保存される

危険度 Info

iOS

・想定される影響

有効なセッションIDが漏えいした場合、正規のユーザになりすました攻撃者によってサービスを不正に利用される可能性がある。

・解説

本アプリケーションでは、セッションIDが端末内のローカルファイルに平文で保存される。このため、仮に攻撃者により端末に物理的にアクセスされファイルを参照された場合、セッションIDが漏えいする可能性がある。

▼事例. セッションID(Bearer)
以下は、サーバ(stg.coupons-api.zensho.com、map-api.zensho.com)との間で利用されているセッションID(Bearer)が平文で保存されるローカルファイルの該当箇所である。

[<Application Home>/Library/jp.co.zensho.olivenooka.stg.plistの内容(抜粋)]

```
<key>login_token</key>
<string>3113adeb24f830054f14345846a87b1d21868235b8a15c3fc85dde5747a972ca</string>
```

▼対象
<Application Home>/Library/jp.co.zensho.olivenooka.stg.plist

・対策

以下のいずれかの対策を実施する。

- 端末内に認証情報を保存しないようにする
- 端末内に認証情報を保存する場合は、平文ではなく暗号化して保存する
- アプリケーションの終了時などに該当するローカルファイルを削除する
- アプリケーション領域内に保存せずkeychainに保存する

・備考

－

報告番号:«ZNSH-app-12»

[13] ログアウト機能の欠如

危険度 Info

iOS

・想定される影響

有効なセッションIDが漏えいした場合、正規のユーザになりすました攻撃者によってサービスを不正に利用される可能性がある。

・解説

本アプリケーションに実装されているログアウト処理に不備がある。

本アプリケーションにはログイン機能が実装されているものの、ログアウト機能は実装されておらず、ユーザが明示的にログアウトすることができない。このため、何らかの原因でセッションIDが漏えいした場合、そのセッションIDを用いてサーバにアクセスされることで、正規のユーザになりすましてサービスを不正に利用される可能性がある。

▼対象
アプリケーション全体

・対策

ユーザが明示的にセッションを無効にできるよう、ログアウト機能を実装する。

・備考

–

報告番号:«ZNSH-app-13»

[14] 端末内に重要情報などを含むスナップショットを保存

危険度 Info

iOS

・想定される影響

重要情報を含むスナップショットが端末内に保存されるため、端末を盗まれるなどした際にそれらの情報が漏えいする可能性がある。

・解説

本アプリケーションをバックグラウンドに移行した際に、移行直前に表示していた画面のスナップショットが端末内に保存される。このため、バックグラウンドへの移行直前の画面にメールアドレスや電話番号などの重要情報が表示されていた場合に、これらの情報がスナップショットに含まれる可能性がある。

以下は、重要情報がスナップショットとして保存される画面である。
[新規登録]
　メールアドレス
[新規登録　メールアドレス認証]
　メールアドレス
[新規登録　メールアドレス認証　プロフィールを登録する]
　性別、お住まいの地域
[ログイン]
　メールアドレス
[サイドバーメニュー　その他　メールアドレス変更]
　メールアドレス
[サイドバーメニュー　その他　お客様情報]
　性別、お住まいの地域
[サイドバーメニュー　その他　ポイントの移行]
　ポイント移行用のID
[テイクアウト弁当WEB注文　連絡先を入力]
　お名前、メールアドレス、電話番号
[テイクアウト弁当WEB注文　連絡先を入力　入力内容のご確認]
　お名前、メールアドレス、電話番号

▼対象
<Application Home>/Library/SplashBoard/Snapshots/sceneID%3Ajp.co.zensho.olivenooka.stg-default/E26B4C46-A167-4C54-8A56-F24C2D4C74A1@3x.ktx
<Application Home>/Library/SplashBoard/Snapshots/sceneID%3Ajp.co.zensho.olivenooka.stg-default/downscaled/0E7BA265-26A1-4372-A96E-2EA3167A6208@3x.ktx
※ファイル名は都度異なる

・対策

アプリケーションをバックグラウンドに移行する際に、以下の対策を実施する。

- 重要情報が表示されたフィールドのhiddenプロパティをYESに設定する
- View全体を別のViewで上書きする

・備考

報告した箇所以外でも同様の問題が発生する可能性があるため、対策する際は全体を見直すことを推奨する。

報告番号:«ZNSH-app-14»

[15] 不必要な画面遷移

危険度 Info

iOS

・想定される影響

- ユーザが入力した情報がローカルファイルに平文で保存される可能性がある
- 不正なサイトへアクセスする可能性がある

・解説

サービス外のWebページを本アプリケーションのWebViewに表示可能である。

本アプリケーションでは、オリーブの丘のWebページ(www.olivenooka.jp)に表示されているSNSアカウントのリンクなどから任意のWebページを本アプリケーションのWebView上で表示できる。このため、WebViewに表示されたWebページ上で検索文字列や認証に利用する文字列を入力すると、それらの情報がローカルファイルに意図せず保存される可能性がある。また、ブラウザとは異なりWebViewでは表示されるサイトのURLは画面に表示されず、ユーザが不正なサイトにアクセスしたことに気づきにくいため、フィッシングなどの被害を受ける可能性もある。

▼対象
ホーム バナー（広告）オリーブの丘(Webページ)
ホーム お持ち帰り注文 公式サイトへ
ホーム オリーブの丘は毎日10:00オープン!
ホーム コンセプト
ホーム メニュー
ホーム お持ち帰りメニュー
ホーム Uber Eats
ホーム 出前館
ホーム アルバイトスタッフ大募集！
メニュー　オリーブの丘(Webページ)
会員証　「?」アイコン　詳しい内容はHPをご確認ください。
店舗検索　お近くの店舗／店舗を調べる　オリーブの丘(Webページ)
ハンバーガーメニュー　よくある質問
ハンバーガーメニュー　その他のお問い合わせ
ハンバーガーメニュー　利用規約
ハンバーガーメニュー　個人情報保護方針

・対策

本アプリケーションのWebViewに表示するアクセス先URLを制限する。又は、本アプリケーションのサービスに不必要なURLについてはブラウザを利用する。

・備考

記載した対象以外でも同様の問題が発生する可能性があるため全体を見直すことを推奨する。

報告番号:«ZNSH-app-15»

[16] 実行ファイル内に内部パスが含まれている

危険度 Info

iOS

- 想定される影響

アプリケーションを解析された際にビルド時の開発環境の内部パスが判明するため、開発環境に関する情報が漏えいする可能性がある。

- 解説

本アプリケーションでは、インストール後に展開された実行ファイルに開発環境の内部パスが含まれている。この内部パスには、本アプリケーションのビルドで使用されたPCのログインアカウントが含まれている可能性があるため、攻撃者に実行ファイルを解析されるとアカウント情報が漏えいする。

以下は、開発環境の内部パスが出力された実行ファイルの該当箇所である。

[<IPA>/Olivenooka_Stg.app/Olivenooka_Stgから抽出した文字列(抜粋)]

```
/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Splash/Controller/ONSplashViewController.swift
/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Other/Controller/ONOtherViewController.swift
/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/Common/Controller/BaseViewController.swift
/Users/ductt7411/Documents/APP/ON/Olivenooka/ViewControllers/NewBackup/View/ONGuideBackupViewController.swift
```

▼対象
<IPA>/Olivenooka_Stg.app/Olivenooka_Stg
<IPA>/Frameworks/Alamofire.framework/Alamofire
<IPA>/Frameworks/DeviceKit.framework/DeviceKit
<IPA>/Frameworks/FBLPromises.framework/FBLPromises
<IPA>/Frameworks/FirebaseCore.framework/FirebaseCore
<IPA>/Frameworks/FirebaseCoreDiagnostics.framework/FirebaseCoreDiagnostics
<IPA>/Frameworks/FirebaseCrashlytics.framework/FirebaseCrashlytics
<IPA>/Frameworks/FirebaseInstallations.framework/FirebaseInstallations
<IPA>/Frameworks/FirebaseInstanceID.framework/FirebaseInstanceID
<IPA>/Frameworks/FirebaseMessaging.framework/FirebaseMessaging
<IPA>/Frameworks/Gifu.framework/Gifu
<IPA>/Frameworks/GoogleDataTransport.framework/GoogleDataTransport
<IPA>/Frameworks/GoogleUtilities.framework/GoogleUtilities
<IPA>/Frameworks/ImageSlideshow.framework/ImageSlideshow
<IPA>/Frameworks/IQKeyboardManagerSwift.framework/IQKeyboardManagerSwift
<IPA>/Frameworks/MBProgressHUD.framework/MBProgressHUD
<IPA>/Frameworks/Moya.framework/Moya
<IPA>/Frameworks/nanopb.framework/nanopb
<IPA>/Frameworks/Parchment.framework/Parchment
<IPA>/Frameworks/SDWebImage.framework/SDWebImage
<IPA>/Frameworks/SecureDefaults.framework/SecureDefaults
<IPA>/Frameworks/SnapKit.framework/SnapKit
<IPA>/Frameworks/SwiftDate.framework/SwiftDate
<IPA>/Frameworks/SwiftyJSON.framework/SwiftyJSON
<IPA>/Frameworks/YLProgressBar.framework/YLProgressBar

・対策

実行ファイルに開発環境の内部パスを含めないため、以下の対策を実施する。
- XcodeのビルドオプションのOther_c_flagsに-DNDEBUG=1を設定する
- Debugではなく、Releaseでビルドする
- ビルド時にアサーションに関するメソッドをコメントまたはマクロで制御する

ただし、Xcodeの他の設定や環境に依存する場合もあるため、上記の設定をしても対策できない可能性がある。対策が困難な場合は、漏えいしても影響がないPCのアカウントを利用してビルドする。

・備考

－

報告番号:«ZNSH-app-16»

[17] 開発時の情報を保存及び内包

危険度 Info

iOS

・想定される影響

実行ファイルにハードコードされている順番待ちQRコードが漏えいすることで不正利用される可能性がある。

・解説

本アプリケーションの実行ファイルには、待ち順確認用のQRコードとして利用される文字列がハードコードされている。このため、実行ファイルを解析された場合に該当情報が漏えいする可能がある。

▼事例. 待ち順確認用のQRコード
以下は、待ち順確認用のQRコードとして利用される文字列が実行ファイルにハードコードされている該当箇所である。
[<IPA>/Olivenooka_Stg.app/Olivenooka_Stg内容(抜粋)]

qr=ZNV941900000000000000000000202212091541

サーバ(stag-api.z-navi.com)に問い合わせて上記値の有効性を確認した結果、無効の結果を得られたが将来的に有効値として利用されている場合も考えられる。

▼対象
<IPA>/Olivenooka_Stg.app/Olivenooka_Stg

・対策

リリース版のアプリケーションにおいて不要な情報やファイルは削除する。

・備考

–

5. おわりに

「サイバー攻撃」という言葉が日常のようにマスメディアに流れ、その攻撃の頻度も巧妙さも日々激しさを増している昨今、そして、情報機器だけではなく、すべてのものがインターネットにつながっていく今日では、そのインターネット越しの脅威について、常に情報を注視し、適切な対応を取り、予防策を講じておくことの重要性も日増しに高まっています。

2014年には「サイバー基本法」も制定され、国や我々の日常生活の基盤を担うような事業者(重要インフラ事業者)には、その対策の実施が義務付けられていますが、国民一人一人に対しても、その重要性の理解と努力が求められています。

そのような背景のもと、今回のセキュリティ診断結果が、貴社システムの安全性を高めるため、またその維持のために、十分にご活用いただけることを願っております。

なお、今回実施させていただいたセキュリティ診断は、ブラックボックステストという特性上、ご報告事象の再現性や網羅性を完全に保証するものでない点、ご承知おきいただきますようお願い致します。また、本報告書の内容は、診断実施時点の情報に基づいておりますが、先述のとおりサイバー攻撃の手法も日進月歩であり、今日安全であるものが明日も安全であり続ける保障はない点も、ご認識おきをお願い致します。セキュアなシステムを維持するために、最新のセキュリティ情報の入手、パッチの適用、セキュリティ診断の定期的な実施、継続的な不正アクセスの監視などを、ぜひ継続的に実施いただければと思います。

末筆ながら、今回のセキュリティ診断の実施に際しご協力をいただきましたことを、ご関係のみなさまに深く感謝致します。

診断結果及び報告書記載内容に関するお問い合わせを受け付けております。

sec-support@d.mbsd.jp

不明点やご質問がありましたら、お気軽にご連絡ください。

Appendix.1 診断項目一覧

[Android/iOS]

診断項目		診断内容詳細
アプリケーション間連携		
	アクセス制限 情報の送受信	不正なアプリケーションからのアクセスを適切に制限しているか 不正な情報を受信することにより情報漏えいや改ざんが発生しないか 重要情報を不適切な方法で送信していないか
通信		
	プロトコル	どのようなプロトコルを用いて通信をしているか
	暗号化の有無	重要情報を送受信する際に暗号化通信をしているか
	サーバ証明書検証	SSL/TLS 通信時にサーバ証明書を検証しているか
	通信内容	個人情報や認証情報等の重要情報を送受信しているか
	プライバシーの保護	適切な許諾を得ずに個人情報などをサーバに送信していないか
認証		
	認証機能	認証機能が安全に実装されているか
	連携機能	アプリケーション連携により認証・認可情報が窃取されないか
	ログアウト機能	ログアウト機能が適切に実装されているか
端末内のデータの取扱		
	保存場所	共有領域に重要情報を保存していないか
	アクセス権限	ファイルへのアクセス権限が適切に設定されているか
	保存方法	重要情報を保存する際に暗号化をしているか
	保存期間	適切なタイミングで端末内の情報を削除しているか
アプリケーションファイル・ログ		
	不要な情報の有無	開発環境やテスト環境、開発者に関連する情報が残存していないか
	不要な情報の出力有無	重要情報や解析の手がかりとなりうる情報を出力してい

		ないか
機能の利用		
	パーミッション設定	アプリケーションが利用しない不要なパーミッションを登録していないか

Appendix.2 危険度判定基準

[Android/iOS]

危険度	想定される被害	具体例
High	外部デバイスからのネットワーク経由の攻撃により、重要情報が漏えいする	アプリケーションが起動したサーバが、ネットワーク経由の攻撃を受け、重要情報が漏えいしてしまう
	サードパーティー製アプリケーションからの攻撃により、他のアプリケーションが扱う情報が漏えいする。または、サービスの利用に影響を及ぼす	アプリケーションを起点として、他のアプリケーションの重要情報が漏えいしてしまう
	機能制限を解除し、不正にアプリケーションを利用される	無料版アプリケーションの機能制限を解除し、有料版機能を不正に利用できてしまう
Medium	サードパーティー製アプリケーションからの攻撃により、重要情報が漏えいする	他のアプリケーションから重要情報が読み込み可能な状態になっている
	連携機能利用時にサードパーティー製アプリケーションに重要情報が漏えいする	アプリケーションが重要情報を暗黙的にブロードキャスト送信している
	中間者攻撃（通信の盗聴など）により重要情報が漏えいする	重要情報を平文で送信している SSL/TLS 通信時にサーバ証明書を適切に検証していない
Low	端末に直接触れることができる攻撃者により、端末内の重要情報が漏えいする	重要情報を暗号化せずに端末内やログに保存している
	サードパーティー製アプリケーションからの攻撃により、アプリケーション上に不正な情報を表示される	不正なアプリケーションから受け取った情報をダイアログや通知などに表示している
Info	直接的な被害に結びつく可能性は低いものの、修正することが望ましい事象	アプリケーションを解析する際の手がかりになる情報などをハードコードしている